IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 22, 2016, accepted July 26, 2016, date of publication April 12, 2017, date of current version June 7, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2693260

The Unfitness of Traditional Military Thinking in Cyber

Four Cyber Tenets That Undermine Conventional Strategies

JAN KALLBERG AND THOMAS S. COOK
Army Cyber Institute, West Point United States Military Academy, West Point, NY 10996, USA
Corresponding author: Jan Kallberg (jan.kallberg@usma.edu)

ABSTRACT Comprehensive theories of conflict in the cyber world have not yet been developed, but the utilization of traditional military strategy and operational concepts in lieu of existing strategies in this realm can mislead, resulting in spurious assessments and unfavorable outcomes. Four tenets of the cyber world present profound challenges for the application of traditional military strategies in cyber conflicts. The cyber world is characterized by the following: 1) a lack of object permanence, which undermines the concept of maneuver; 2) limited or absent measurement of effectiveness in offensive cyber; 3) conflicts that are executed at computational speed, thus removing the time window for meaningful strategic leadership; and 4) anonymity, which makes the parties to the conflict unknown. As a result, the use of traditional military thinking and path-dependent behavior in cyber is likely to lead to incorrect conclusions regarding strategic achievements and abilities in the pre-conflict stage, and increase the risk of strategic failure during conflict and provide an opportunity for an adversary's strategic surprise.

INDEX TERMS Cyber operations, cyber defense, offensive cyber operations, information operations.

I. INTRODUCTION

Recent applications of traditional military strategy [1] and operational concepts in the arena of cyber conflict have shown that this approach can be misleading and generate spurious assessments and unfavorable outcomes.

On the other hand, theories for application in the cyber context have not yet been developed. The questionable fit of traditional strategies and the need for cyber-specific strategies is apparent when considering four tenets of the cyber world that challenge the effectiveness of traditional military strategies and thoughts.

The cyber world is characterized by the following: 1) a lack of object permanence, which undermines the concept of maneuver; 2) limited or absent measurement of effectiveness in offensive cyber; 3) conflicts that are executed at computational speed, removing the time window that would allow for meaningful strategic leadership; and 4) anonymity that makes the parties to the conflict unsure who is the other party. Anonymity leads to confusion and can lead to unwanted escalation due to inability to separate foe and neutral party. As a result, the application of traditional military thinking in cyber is likely to lead to incorrect conclusions regarding strategic achievements and abilities in the pre-conflict stage, increasing the risk of strategic failure in actual conflict.

Military establishments have been fight war in a specific way for centuries, there is an order of battle, command and control, and an executive leadership. The way combat is directed and led is challenged by cyber with an ever-evolving battlefield, interchanges at machine speed, and as the contour of the future indicates a very short time-window in actual engagements for human decision-making.

As noted military strategist Edward N. Luttwak once stated, strategies without the ability to execute are pointless exercises [2]. Established military thinking is appealing as an explanatory model for the outfall of cyber conflicts for two reasons. First, it is already in place. For generations, the training and education of military officers, political scientists, and the political elite have focused on the works of Carl von Clausewitz, Sun Tzu, Antoine-Henri Jomini, B. H. Liddell-Hart, Heinz Guderian, and other traditional thinkers whose theories are considered timeless and universal. This common historical focus on path dependency that renders political, institutional, and bureaucratic organizations unable to adapt under the pressure of change has been studied thoroughly [3].

Second, because alternative strategic theories explicitly for cyber have not been established, traditional military thinking becomes the default formulator of strategy [4], [5]. In fact,

in some quarters, the concepts of cyber war (and cyber conflicts leading to war) have been rejected under the belief that they do not fit traditional military thinking, and thus do not meet the traditional military framework for destruction and capture of physical items [6]. Over time, domain-specific strategic fundamentals for cyber will emerge based on the experiences and inferences identified in a major cyber conflict. While the lack of major nation/state cyber conflicts to date has delayed the development of cyber theory, an identification of the unique characteristics of cyber prior to this provides a foundation for strategic development in this realm.

II. TENET 1 - OBJECT PERMANENCE

One major challenge in the application of traditional military thinking to cyberspace is object permanence. The main body of traditional military thinking was consolidated under the framework of the art of war during the Napoleonic era of the late 18th and early 19th centuries. At that time, the major nation states created war colleges and adopted a scientific approach under which warfare was analyzed and taught using systematic and replicable theories on campaign tactics that would most often lead to victory.

From these theories emerged detailed types of battlefield maneuvers, orders of battle, and strategies for achieving superiority by improving one's position for firing on the enemy and reaching a decisive outcome.

In the early 1800s, it was inconceivable that objects could appear, disappear, reappear, or change form at computational speed. Today, however, the cyber environment is emerging, changing, and evolving without any positions fixed to assets that persist over time. Information has no (or little) time-bound linear context.

Under traditional military thinking, for example, the concept of maneuver is pivotal for how one arranges for and conducts battle, and for tactical considerations in determining positions for firing at the enemy to reduce the enemy's options, strength, and initiative. Thus, Napoleonic generals operated under a framework in which they could decide where to fight the battle, overlook the potential battle field, draw maps, discuss the order of battle, arrange troops and give orders to start at dawn, and otherwise conduct the battle according to plans that leveraged the physical terrain and increased the likelihood of success. Likewise, modern concepts such as *Blitzkrieg*, the armored assault that overruns the infantry and strikes deep in the rear echelons, also requires object permanence [7].

In cyberspace, however, one can create, change, move, duplicate and delete objects at machine speed as long as there are assets to support the digital engagement. The only object permanence that exists in the cyber infrastructure supports the cyber war effort through server centers, cables, drones, power sources, and antennas. The execution of cyber war occurs in the information and perception space, where object permanence is limited or non-existent [8].

III. TENET 2 - MEASUREMENT OF EFFECTIVENESS

An attacker in cyber space has limited ability to verify, assess, and act based on information gleaned from a previous attack and its aftermath. Since the invention of the bow and arrow in prehistoric times, armies have fought from a distance by firing weapons, observing the results of this action, and adjusting their aim to maximize the lethal effect on the targeted enemy. In cyber battles, damage is hidden under layers of sophisticated networks and, increasingly, through a kaleidoscope of nodes and digital interchanges. Even if limited measures can be established, the accuracy of the data is troublesome to validate, if possible, and spurious assessments are a major risk.

The attacker can see parts of the effect, performance data can be captured, aggregated, and analyzed to create an understanding of the unfolding events in the targeted systems, but the picture is not clear and there are still major uncertainties of the actual effect.

The French Napoleonic general storming the thin red line of British troops could see with his own eyes how the enemy's lines became thinner following each rifle volley. He received an accurate measurement of effectiveness in real time, forcing a retreat if the British remained standing after the French Guards lost their battlefield thrust. In this context, measurable results provide the information necessary for further decision-making and battle assessment.

The cyber world lacks an accurate feedback loop of quantifiable results, and has limited measure of effectiveness and no chain of events that culminates at a decisive moment [9].

A defender is in a stronger position to measure the effectiveness of the defenses because of the ability to implement frameworks to assess operational stability, level of degraded operations, and where and how internal defensive measures have been engaged. The defending actor can see their own networks and get at least a crude understanding of the impact from the cyber engagement. The measurement of effectiveness problem is most challenging in offensive cyber operations or any aggressive cyber interchange where the outbound engagement will face the inability to properly assess impact and effectiveness [10].

IV. TENET 3 - COMPUTATIONAL SPEED EXECUTION

Military units are designed for leadership under a single officer, who, through the support of technical systems and information, assesses the situation, makes decisions, and determines future courses of action. Top-echelon military leadership executes national defense strategies through a political process that takes time. As an example, smaller tactical decisions might need five minutes; operational decisions, fifty minutes; and strategic preauthorized decisions, five hours. Grander strategic moves might require political deliberations that last five days.

The question today is, can cyber, as an area of conflict, operate and allow leadership interaction within these traditional periods, or will future cyber conflict execute far too

quickly for involvement by leadership at any level other than lowest and most tactical?

If these conditions provide tactical input only, the cyber engagement risks losing its structure and becoming a chain of reactions to ongoing events without the possibility of major coordination or strategic intent?

Rapidly executed cyber attacks — especially those that are well prepared, organized, and premeditated — eliminate the ability to mount a cyber defense, because the short time available for decision making restricts decisions to the tactical level. One analogy for fighting without access to command and control is the air defenses without access to ground control, or the Airborne Warning and Control System (AWACS) command, under which pilots of armed fighter jets are instructed to make all tactical decisions without coordination or control in relation to other defense assets, including the decision to fire at will.

Even if we solved the other challenges — lack of object permanence, lack of measureable results, and anonymity — the issue of computerized machine speed, in which premeditated systematic cyber attacks render the influence of human leadership impossible, would dominate. In reality, Cyber attacks would be over before leadership could identify and understand the strategic landscape. If the attacks were not premeditated, but relied on harvesting vulnerabilities in an ongoing conflict, the time frames in which larger, future engagements could occur limit (or in the worst case, nullify) the orchestration of a cyber defense.

V. TENET 4 - ANONYMITY

The tenet of anonymity is well researched and understood as a complicating factor in cyber operations. The lack of proper identification in cyberspace undermines one's ability to engage [11]. Anonymity also increases the risk of friendly fire in cyber, in which entities engage friendly targets [12] due to their inability to distinguish between friend and foe at computational speeds.

Adding to this complexity is the use of proxies in cyber operations [13]. Several countries in the developing world have a growing internet presence and commercial computer capacity, but their focus is on economic growth and satisfying an emerging market, and security concerns are not properly addressed. Engagements in a militarized domain are likely to utilize routing and attack vectors that supports anonymity and hinders accurate accountability or delays determining the actual digital locale of attacker. There are several tools and techniques available [14] and the tools are expanding in ability and accessibility. The conventional way to preserve anonymity by proxy servers, utilizing delay tolerant networks [15], TOR packages, and Onion networks do not require any major investment. These techniques are available even for unsophisticated actors. An advanced offensive cyber attacker has in his reach numerous options to ensure that traceability in undermined and the highest level of a defender's ability to determine who the attacker is becomes a plausible certainty. The question, and that is a decision for the defender, if plausible is enough to warrant counter-strikes and other repercussions.

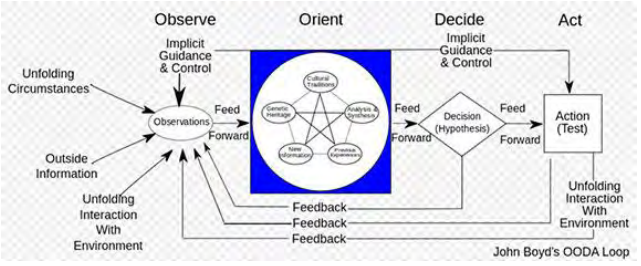


FIGURE 1. "OODA Boyd" by Patrick Edwin Moran - Own work. Licensed under CC BY 3.0 via Wikimedia Commons.

Anonymous attacks could trigger counter-attacks on assumed plausible opponents, guilty or not, and lead to uncontrolled escalation. Traditional military thinking is based on targeting of verified hostile units or objects. The cyber tenet of anonymity prevents a decision maker from a clear picture who they are engaging. In traditional terms, engagements with plausible enemies are like opening fire on shadows in the fog of war, which can disintegrate the order on the battlefield and lead to entropy of the battle.

VI. COMMAND AND CONTROL

In principle, military command and control (C2) follows the steps of observe, orient, decide, act, as described in the OODA (Observe, Orient, Decide, Act) loop developed by John Boyd in the 1960s (Fig. 1) [16].

The OODA loop requires the ability to assess ongoing events (as in the initial step of ''Observe''), but under conditions of anonymity, computational speed in cyber execution, and lack of object permanence, the observations feeding the loop are likely to be inaccurate, if not spurious.

The ''Orient'' stage in the OODA loop — reaction to unfolding events and positioning for better outcome — assumes a maneuver space with favorable positions, but the lack of object permanence in cyber brings and ever-changing battle field and permanent disorientation rather than re-orientation. If the ''Observe'' and ''Orient'' stages are not relevant to the factual engagements, then it is likely that the ''Decide'' stage will fail to deliver the proper course of action and thus lead to ineffective ''Act'' stage.

Computational speed exacerbates the inability to assess and act, and the increasingly shortened time frames likely to be found in future cyber conflicts will disallow any significant human deliberation. The lack of object permanence undermines the ability to ''Orient'', the limited measurement of effectiveness removes the feedback loop and the anonymity removes the ability to clearly understand circumstances, outside information, and assess unfolding interaction with the environment. The four cyber specific tenets weaken traditional command and control, which is pivotal to established military strategies.

VII. CYBER OPERATIONS AS A MERE ENABLER OF WAR

The main counterargument against the need to develop cyber-unique strategies and concepts is the redefining of cyber

operations as an enabler of war, and not a distinct form of war itself. If that is true, then the four tenets are not of any major concerns because cyber is limited to a supporting role. When cyber operations are considered merely tools that enable other military operations, and are not utilized as a weapon of strategic intent, then cyber operations will be integrated in the grander strategy executed [17] and there will be no need for cyber operations strategies for decisive outcomes in an exclusively cyber warfighting domain [18].

The weakness in the argument that reduces cyber operations to an enabler of either traditional weapons or traditional forms of war, and not a form of war itself, is cyber's relevance over time. As time progress, the position weakens further.

It is highly likely that cyber operations and the ability to conduct a conflict in cyberspace will escalate and become more sophisticated over time. The belief that cyber is peripheral to war, and not a discrete form of warfare, assumes that wars are fought under conditions that are permanent.

History has shown with sufficient clarity that warfighting abilities constantly emerge, develop and change. The assumption that the characteristics of the surrounding environment are static has repeatedly led to horrifying defeats. The French disaster of June 1940, for example, was largely the result of the French refusal to conduct armored warfare. Even if French tanks had outnumbered German tanks, the refusal had direct tactical implications. The French considered tanks to be peripheral, mere enablers for the infantry. To the French, tanks were primarily fire support vehicles for the infantry, or transportable machine gun nests, and the French High Command prohibited tanks from operating independently of the infantry. The fact that no radio communication existed between French tanks reflects the assumption that such coordination was unnecessary because tanks merely followed the infantry. As battles started to unfold, and French commanders realized the need to engage German tanks, the French tanks were at a significant disadvantage without radio communication and guns designed to deliver high-explosive rounds to support infantry, instead of armor-piercing munitions appropriate for tank-on-tank battles.

The line of thought that tanks were simply support for the infantry created a path dependency, so that even after realizing the mistake, the limitations could not be overcome and the German armored divisions could not be engaged.

A refusal to consider cyber weapons a freestanding form of war, and instead force them into the concepts and formations of the past, could eliminate the opportunity embedded in these capabilities, analogous to the French army's failure in 1940 to utilize armor. The path-dependent approach of seeking to impose new weapons on an earlier form of war removes the strategic surprise and supremacy of a revolution in military affairs [19].

VIII. CYBER STRATEGY

Each strategy has a fundamental framework that explains why things are the way we perceive them, structures assumptions for how they operate, and provides clues on how to reach strategic goals. Strategy, therefore, is theory based, with theory providing the intellectual underpinnings for predicting the outcomes leading to the end goal that the strategy pursues. Traditional military thinking faces serious challenges today, generating questions regarding the applicability of established military strategies in cyber, and whether, if these strategies are applied, they could lead to defeat instead of a decisive, positive outcome.

Cyber is no longer a mere enabler of joint operations, but instead a viable strategic option for confronting adversarial societies. The current alternative to strategic cyber is to attack the adversary using cyber, when exploitation opportunities occur. This is likely to degrade parts of the information infrastructure, and will not achieve any strategic goals. If an adversarial societal compound is unaffected by a cyber conflict, the conflict itself has not reached a decisive outcome, and the only possible results are escalation of a tit-for-tat game or a stalemate.

Decisive outcomes lead to policy change through partial or full submission to foreign will by the targeted society [9]. The decisive outcome in cyber is reached either by removing military capacity using cyber attacks or by destabilizing the targeted society. The removal of military capacity is likely temporary, followed by software coding that closes these limited vulnerabilities, compared to societal destabilization that jeopardizes the entire regime. Cyber thus becomes a high-velocity realm of engagement that marginalizes human leadership when engagement is ongoing. Computers at war engage at computational, not human, speed.

IX. CONCLUSION

The assumption that leadership always operates with sufficient capabilities is an illusion that could result in poor judgment and grave errors; those who question and assess their capabilities more often have favorable outcomes. The application of traditional military principles to strategic decision-making in cyber conflicts assumes a battle space that is largely absent in cyber space. As cyber evolves as a battle space and contested area, new innovative strategic principles for this realm must be developed to address the core four tenets of cyber combat: 1) lack of object permanence, 2) lack of relevant measurement of effectiveness, 3) computational speed in execution, and 4) anonymity.

Cyber-relevant strategies are likely to become increasingly reliant on artificial intelligence and preset action items, such as computational speed in execution and a situational awareness that assesses contested cyber space in real time, and where nodes and cyber terrain are created and deleted, as humans become increasingly unable to understand an engagement as it develops. The application of traditional military principles in strategic decision-making in cyber conflicts assumes a battle space that, to a high degree, are absent in cyber space. As cyber evolves as a battle space and contested area new, innovative strategic principles for this realm must be developed to address the core four concerning tenets of cyber combat: lack of object permanence, lack of relevant

measurement of effectiveness, computational speed in execution, and anonymity. Cyber-relevant strategies are increasingly likely to rely on artificial intelligence and preset action items as computational speed in execution and a situational awareness that assess contested cyber space in real time, and where nodes and cyber terrain are created and deleted, as humans no longer can effectively understand an engagement as it unfolds.

The assumption that the military, once given adequate training and resources, are predisposed to have sufficient capabilities to lead, engage, and defend can be an illusion that results in poor judgment and grave errors. The traditional military and its structure is in several ways a misfit in cyber, and even if it is shared with other agencies such as police and other law enforcement, but that has not hindered the notion that the traditional military thinking and structures can be credible cyber defenders.

Does it mean that the military should not be used in cyber? No, but the uniqueness of cyber limits the ability to be successful as a military cyber defender unless changes are made to adapt to a new fighting environment radically different from the battle space that created traditional military thinking. The future cyber forces need to be able to operate in an environment with lack of object permanence, limited of relevant measurement of effectiveness, computational speed in execution, and a to a high degree anonymous actors. Then, cyber as an area of conflict will require unorthodox approaches, innovation, and an ability to look beyond how we are used to organize defenses.

ACKNOWLEDGEMENT

The views expressed herein are those of the author and do not reflect the official policy or position of the Army Cyber Institute, the United States Military Academy, the Department of the Army, or the Department of Defense.

REFERENCES

[1] B. K. Rios, "Sun Tzu was a hacker: An examination of the tactics and operations from a real world cyber attack," *The Virtual Battlefield: Perspectives on Cyber Warfare*, vol. 3, C. Czosseck and K. Geers, Eds. Amsterdam, The Netherlands: IOS Press, 2009.

[2] E. Luttwak, *The Grand Strategy of the Roman Empire: From the First Century A.D. to the Third*, Baltimore, MD, USA: Johns Hopkins Univ. Press, 1979.

[3] P. Pierson, "Increasing returns, path dependence, and the study of politics," *Amer. Political Sci. Rev.*, vol. 94, no. 2, pp. 251–267, 2000.

[4] K. Geers, "Strategic cyber defense: Which way forward?" *J. Homeland Secur. Emergency Manage.*, vol. 9, no. 11, pp. 1–10, 2002.

[5] T. Rid, "Cyber war will not take place," *J. Strategic Stud.*, vol. 35, no. 1, pp. 5–32, 2012.

[6] C. B. Greathouse, "Cyber war and strategic thought: Do the classic theorists still matter?" in *Cyberspace and International Relations*. Berlin, Germany: Springer, 2014, pp. 21–40.

[7] H. Guderian, *Panzer Leader*, Cambridge, MA: Da Capo Press, 2001.

[8] B. T. Williams, "The joint force commander's guide to cyberspace operations," *Joint Force Quart.*, vol. 73, pp. 12–19, Sep. 2014.

[9] J. Kallberg, "Strategic cyberwar theory—A foundation for designing decisive strategic cyber operations," *Cyber Defense Rev.*, vol. 1, no. 1, pp. 101–116, 2016.

[10] P. E. Black and K. S. M. Souppaya, "Handbook of science and technology for homeland security," *Cyber Security Metrics and Measures*. Hoboken, NJ, USA: Wiley , 2008.

[11] P. C. Reich, S. Weinstein, C. Wild, and A. S. Cabanlong, "Cyber warfare: A review of theories, law, policies, actual incidents—And the dilemma of anonymity," *Eur. J. Law Technol.*, vol. 1, no. 2, 2010. [Online]. Available: http://ejlt.org/article/view/40/58

[12] T. E. Carroll, F. L. Greitzer, and A. D. Roberts, "Security informatics research challenges for mitigating cyber friendly fire," *Secur. Informat.*, vol. 3, no. 1, pp. 1–14, 2014.

[13] J. Kallberg and S. Rowlen, "African nations as proxies in covert cyber operations," *African Secur. Rev.*, vol. 23, no. 3, pp. 307–311, 2014.

[14] P. Syverson, G. Tsudik, M. Reed, and C. Landwehr, "Towards an analysis of onion routing security," in *Designing Privacy Enhancing Technologies*, Berlin, Germany: Springer, 2001, pp. 96–114.

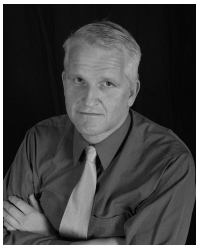
[15] A. Kate, M. Gregory, and U. Hengartner, "Anonymity and security in delay tolerant networks," in *Proc. IEEE 3rd Int. Conf. Secur. Privacy Commun. Netw. Workshops SecureComm*, Sep. 2007, pp. 504–513.

[16] F. P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, Abingdon, U.K.: Routledge, 2007.

[17] C. S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is not Falling*, Carlisle, PA, USA: Army War College—Strategic Studies Institute, 2013.

[18] M. C. Libicki, "Why cyber war will not and should not have its grand strategist," *Strategic Studies Quart.*, vol. 8, no. 1, pp. 23–39, 2014.

[19] J. Kallberg and B. Thuraisingham, "Cyber operations-bridging from concept to cyber superiority," *Joint Forces Quart.*, vol. 68, no. 1, pp. 53–58.



JAN KALLBERG was a researcher with the Cyber Security Research and Education Institute, The University of Texas at Dallas, an Assistant Professor with Arkansas Tech University, and a part-time Faculty Member with George Washington University. He is currently an Assistant Professor in political science with the Department of Social Sciences, United States Military Academy at West Point, and a Research Scientist with the Army Cyber Institute at West Point. He has authored papers in the *Strategic Studies Quarterly*, the *Joint Forces Quarterly*, the *IEEE Professional*, IEEE Access, and IEEE Security and Privacy.

THOMAS S. COOK received the M.S. degree in industrial engineering from the University of Louisville, and the M.S. degree in computer science and the Ph.D. degree in software engineering from the Naval Postgraduate School. He was a commissioned Armor and then joined the Army Acquisition Corporation. He served as the Research Director of the Army Cyber Institute at West Point until transitioning to Assistant Professor with the Department of Electrical Engineering and Computer Science, United States Military Academy. His research focus is software engineering, real-time systems, information assurance, and computer science education.